UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/593,280	06/13/2000	Cheuk W. Ko	NA00-02401	7783

28875 7590 11/20/2003

SILICON VALLEY INTELLECTUAL PROPERTY GROUP
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
HENEGHAN, MATTHEW E	
ART UNIT	**PAPER NUMBER**
2134	5

DATE MAILED: 11/20/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/593,280	KO, CHEUK W.	
	Examiner	Art Unit	
	Matthew Heneghan	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 June 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *13 June 2000* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

*See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. Claims 1-27 have been examined.

Drawings

2. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference sign(s) not mentioned in the description: figure 4, items "400" and "418." A proposed drawing correction, corrected drawings, or amendment to the specification to add the reference sign(s) in the description, are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

3. The drawings are objected to because the "OPERATING SYSTEM" item in figure 2 should be numbered "113," instead of "112." A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Claim Objections

Claims 5, 7, 8, 14, 16, 17, and 26 are objected to because of the following informalities:

Regarding claims 5, 7, 8, 14, 16, and 17, it is unclear whether the limitations following the word "involves" are open-ended or close-ended in scope.

Regarding claim 26, there is no transitional phrase to define whether the recitation of limitations is open-ended or closed-ended in scope.

For the purposes of the prior art search, it is being presumed that all limitations are open-ended.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 4, 6, 13, 15, 20, 22, and 24 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding claims 4, 6, 13, 15, 22, and 24, the phrase "can include" renders the claim indefinite because it is unclear whether the limitation(s) following the phrase are part of the claimed invention. For purposes of the prior art search, the lists of limitations are being treated as Markush groups.

Regarding claim 20, the word "and/or" renders the claim indefinite because it is unclear whether the limitations preceding and following the word part of the claimed invention. For purposes of the prior art search, art is being considered to anticipate the

limitations if it changes one or more auditing criteria OR at least one target attribute OR does both.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1, 2, 8-11, 17-20, 26, and 27 are rejected under 35 U.S.C. 102(b) as being anticipated by U.S Patent No. 5,557,742 to Smaha et al.

As per claims 1, 8, 10, 17, 19, and 26, the intrusion detection system disclosed by Smaha receives an audit trail, stores specified data in an event data structure(60), compares data against the contents of the information modules(62,64,66) using complete query(84) and compares one or more data to criteria for detecting an intrusion (see column 7, lines 8-49). More specifically, a misuse engine is employed that uses queries stored in a signature data structure(108) to determine intrusions (see column 9, line 31 to column 10, line 32).

As per claims 2, 9, 11, 18, 20, and 27, Smaha discloses that programs can be used to dynamically select misuses based on a set of criteria (see column 9, lines 15-20).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 4, 6, 13, 15, 22, and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S Patent No. 5,557,742 to Smaha et al. as applied to claim 1 above, and further in view of U.S. Patent No. 6,584,508 to Epstein et al.

Smaha does not disclose the analysis of other data relevant to logged system calls in the misuse engine.

The data guard system disclosed by Epstein includes the ability to screen a variety of system call attributes by using wrappers around system calls, so that any parameter to the system call may be intercepted (see column 5, lines 32-55). Epstein further discloses that intercepted calls might include an exec call, for which the name of a process is passed as a parameter, or an attempt to read a file, for which a parameter must be an identifier for the calling application program (see column 6, lines 58-67). Epstein further suggests that the software wrappers provide for relatively small specifications of the allowed behavior of associated multi-part proxy components, and security of firewall components is thereby improved (see column 3, lines 29-32).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the intrusion detection system disclosed by Smaha by implementing software wrappers for the system calls, making the parameters of system calls available for auditing, as disclosed by Epstein, thereby improving the security of firewall components.

7. Claims 5, 14, and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S Patent No. 5,557,742 to Smaha et al. as applied to claim 1 above, and further in view of U.S. Patent No. 5,623,601 to Vu.

Smaha does not disclose the incorporation of the misuse engine into the operating system's kernel.

Vu discloses a system for secure gateway communications that includes the incorporation of the engine directly in the operating system kernel (see column 4, lines 51-64), and further notes that data communications are delivered to the application level through the kernel (see column 6, lines 2-13).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to incorporate the misuse engine disclosed by Smaha into the operating system kernel, as disclosed by Vu, as all data communications are delivered to the application level through the kernel.

8. Claims 3, 7, 12, 16, 21, and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S Patent No. 5,557,742 to Smaha et al.

As per claims 3, 12, and 21, Smaha discloses that the signature information structure is initialized in a UNIX™ system by retrieving it from disk storage (see column 12, lines 5-40). Official notice is given that it is well-known in the art that all transactions with disk storage in the UNIX™ operating system are necessarily performed using one of a number of system calls, such as read(), open(), and close().

Smaha does not specifically disclose the use of jump tables for choosing the appropriate system calls for performing file I/O.

Official notice is given that it is well-known in the art that the method of using a jump table is an efficient way, both in terms of execution speed and memory usage, to specify a jump or call to one of a list of processes in a situation where the decision can be made based upon the value of an single integer variable, such as an index, and that jump tables can be dynamically modified, based upon changing conditions.

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to implement the system disclosed by Smaha by using a system call jump table, in order to efficiently choose the correct the correct system call by which to retrieve the signature information structure from disk storage.

As per claims 7, 16, and 25, Smaha does not specifically disclose the filtering of audit logs in order to conserve space.

Official notice is given that the method of filtering unwanted information from a file in order to reduce its size is well-known in the art.

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to further implement the system disclosed by Smaha by filtering unneeded information from the audit log in order to conserve space.

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent No. 5,278,901 to Shieh et al. discloses a system for detecting intrusions using pattern analysis.

U.S. Patent No. 5,485,409 to Gupta et al. discloses a system for analyzing weaknesses in computer systems and includes methods for analyzing incoming system calls.

U.S. Patent No. 5,621,889 to Lermuzeaux et al. discloses a system for analyzing anomalies to detect intrusions.

U.S. Patent No. 6,275,942 to Bernhard et al. discloses a system for responding to system misuses and intrusions.

U.S. Patent No. 6,347,374 to Drake et al. discloses a system for analyzing audit trails for intrusions.

U.S. Patent No. 6,408,391 to Huff et al. discloses a militaristic software package for recognizing and reacting to intrusions.

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew E. Heneghan, whose telephone number is (703) 305-7727. The examiner can normally be reached on Monday-Thursday from 8:00 AM - 4:00 PM Eastern Time. The examiner can also be reached on alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse, can be reached on (703) 308-4789.

Any response to this action should be mailed to:
Commissioner of Patents and Trademarks
Washington, DC 20231
Or faxed to:
(703) 872-9306
Hand-delivered responses should be brought to Crystal Park 2, 2121 Crystal Drive, Arlington, VA 22202, Fourth Floor (Receptionist).

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

MEH

November 13, 2003

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100